AUGMENTING THE ONION

FACILITATING ENHANCED DETECTION AND RESPONSE WITH OPEN SOURCE TOOLS

Wes Lambert

Packet Hacking Village, 2019

ME, MYSELF, AND ONION

- Husband and father of four
  - Co-manager of household operations
- Coffee, Indian food, and FOSS lover
- Senior Engineer, Security Onion Solutions

INTRODUCTION

- Shift from pure prevention to include detection and response.
- Bad guys WILL get in at some point!
- Even the next-nextest-generation firewall won’t save you.

S/PREVENTION/DETECTION/

- When the bad guys get in, we need some way to find them.
- We need to have a way to retrieve data about our network.
- We need data that is easily digestible.
- We need data that provides context around an event.
- We need to build upon NSM and implement enterprise-wide security monitoring.

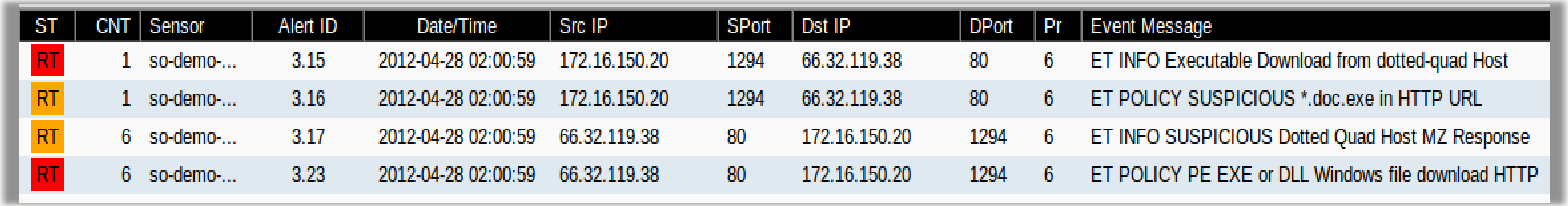
THE (SECURITY) ONION

Open source enterprise security monitoring and log management platform

- **Alert Data** (IDS Alerts) – Snort /Suricata
- **Session Data** (Connections) – Bro
- **Transaction Data** (DNS/FTP/HTTP) - Bro
- **Extracted Content** Data (Files) - Bro
- **Full Content Data** (PCAP) – netsniff-ng
- **Host Data** (Wazuh, Beats, Symon, Autoruns)
- **Alerting** (Email, Slack, Scripts) - Elastalert
- **Data Enrichment and Visualization** (Elastic Stack)

https://securityonion.net

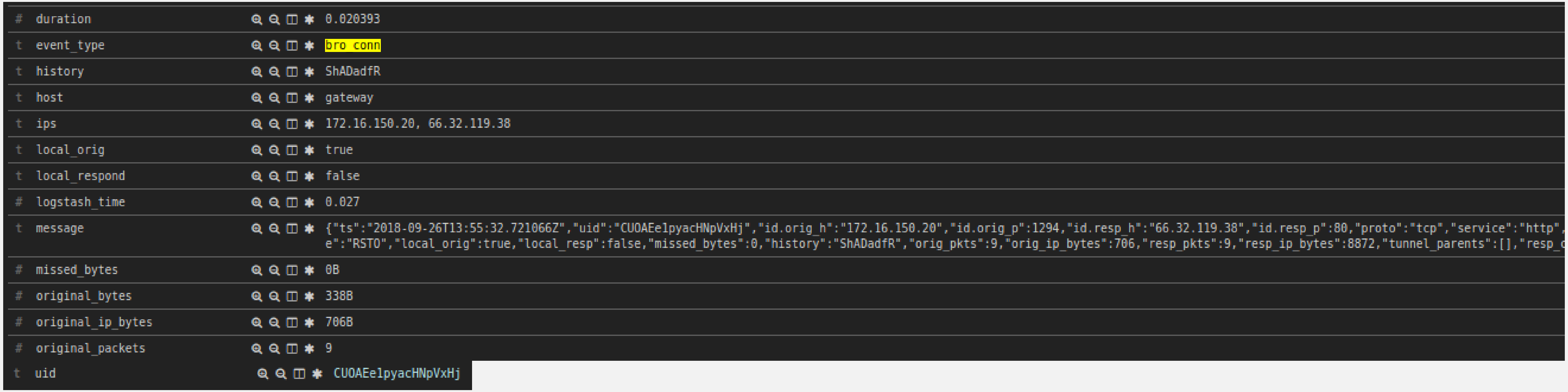
SECURITY ONION – ALERT DATA



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	so-demo-...	3.15	2012-04-28 02:00:59	172.16.150.20	1294	66.32.119.38	80	6	ET INFO Executable Download from dotted-quad Host
RT	1	so-demo-...	3.16	2012-04-28 02:00:59	172.16.150.20	1294	66.32.119.38	80	6	ET POLICY SUSPICIOUS *.doc.exe in HTTP URL
RT	6	so-demo-...	3.17	2012-04-28 02:00:59	66.32.119.38	80	172.16.150.20	1294	6	ET INFO SUSPICIOUS Dotted Quad Host MZ Response
RT	6	so-demo-...	3.23	2012-04-28 02:00:59	66.32.119.38	80	172.16.150.20	1294	6	ET POLICY PE EXE or DLL Windows file download HTTP

- Generated by matching a pre-defined signature that says this is something of which to be aware.
- Tells us something may have happened – further investigation required to determine if something of significance.

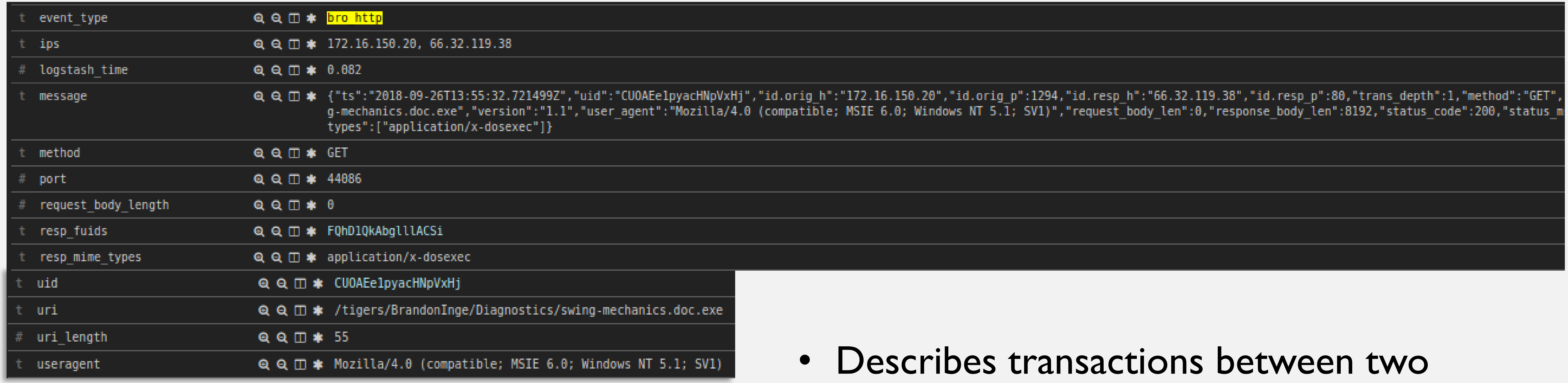
SECURITY ONION – SESSION DATA



```
#  duration             0.020393
t  event_type           bro_conn
t  history              ShADadfR
t  host                 gateway
t  ips                  172.16.150.20, 66.32.119.38
t  local_orig           true
t  local_respond        false
#  logstash_time        0.027
t  message              {"ts":"2018-09-26T13:55:32.721066Z","uid":"CUOAEe1pyacHNpVxHj","id.orig_h":"172.16.150.20","id.orig_p":1294,"id.resp_h":"66.32.119.38","id.resp_p":80,"proto":"tcp","service":"http",
                        e":"RSTO","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"ShADadfR","orig_pkts":9,"orig_ip_bytes":706,"resp_pkts":9,"resp_ip_bytes":8872,"tunnel_parents":[],"resp_
#  missed_bytes         0B
#  original_bytes       338B
#  original_ip_bytes    706B
#  original_packets     9
t  uid                  CUOAEe1pyacHNpVxHj
```

- Summary data, similar to Netflow
- Can identify type of traffic (ex. FTP, HTTP, DNS, etc.)
- Can be used to correlate other activity through the UID

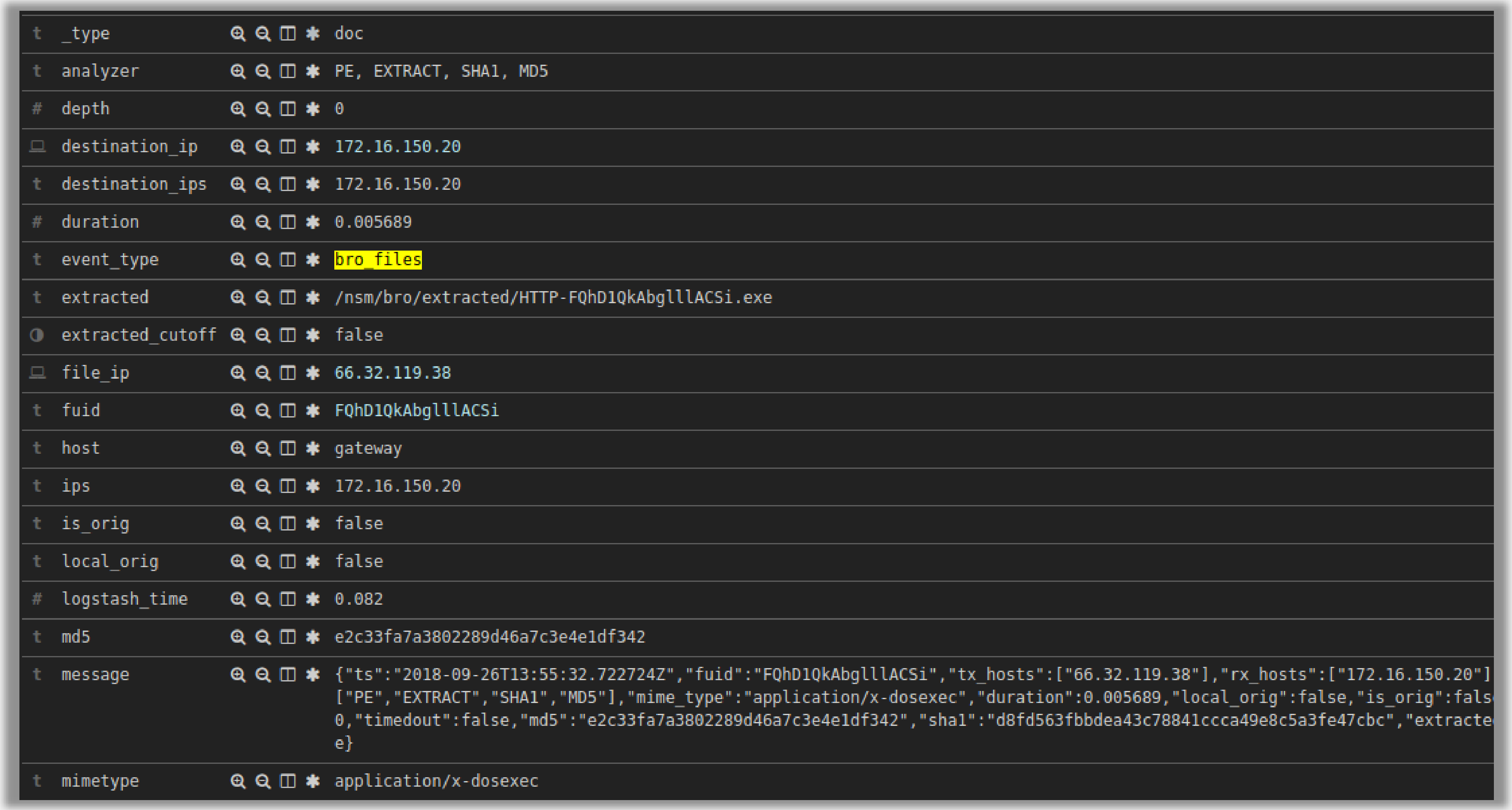
SECURITY ONION – TRANSACTION DATA



```
t  event_type          bro_http
t  ips                 172.16.150.20, 66.32.119.38
#  logstash_time       0.082
t  message             {"ts":"2018-09-26T13:55:32.721499Z","uid":"CUOAEe1pyacHNpVxHj","id.orig_h":"172.16.150.20","id.orig_p":1294,"id.resp_h":"66.32.119.38","id.resp_p":80,"trans_depth":1,"method":"GET",
                       g-mechanics.doc.exe","version":"1.1","user_agent":"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)","request_body_len":0,"response_body_len":8192,"status_code":200,"status_m
                       types":["application/x-dosexec"]}
t  method              GET
#  port                44086
#  request_body_length 0
t  resp_fuids          FQhD1QkAbglllACSi
t  resp_mime_types     application/x-dosexec
t  uid                 CUOAEe1pyacHNpVxHj
t  uri                 /tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe
#  uri_length          55
t  useragent           Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
```

- Describes transactions between two hosts
- In this case, HTTP traffic
- Can tie to a unique FUID (File ID) found in files.log

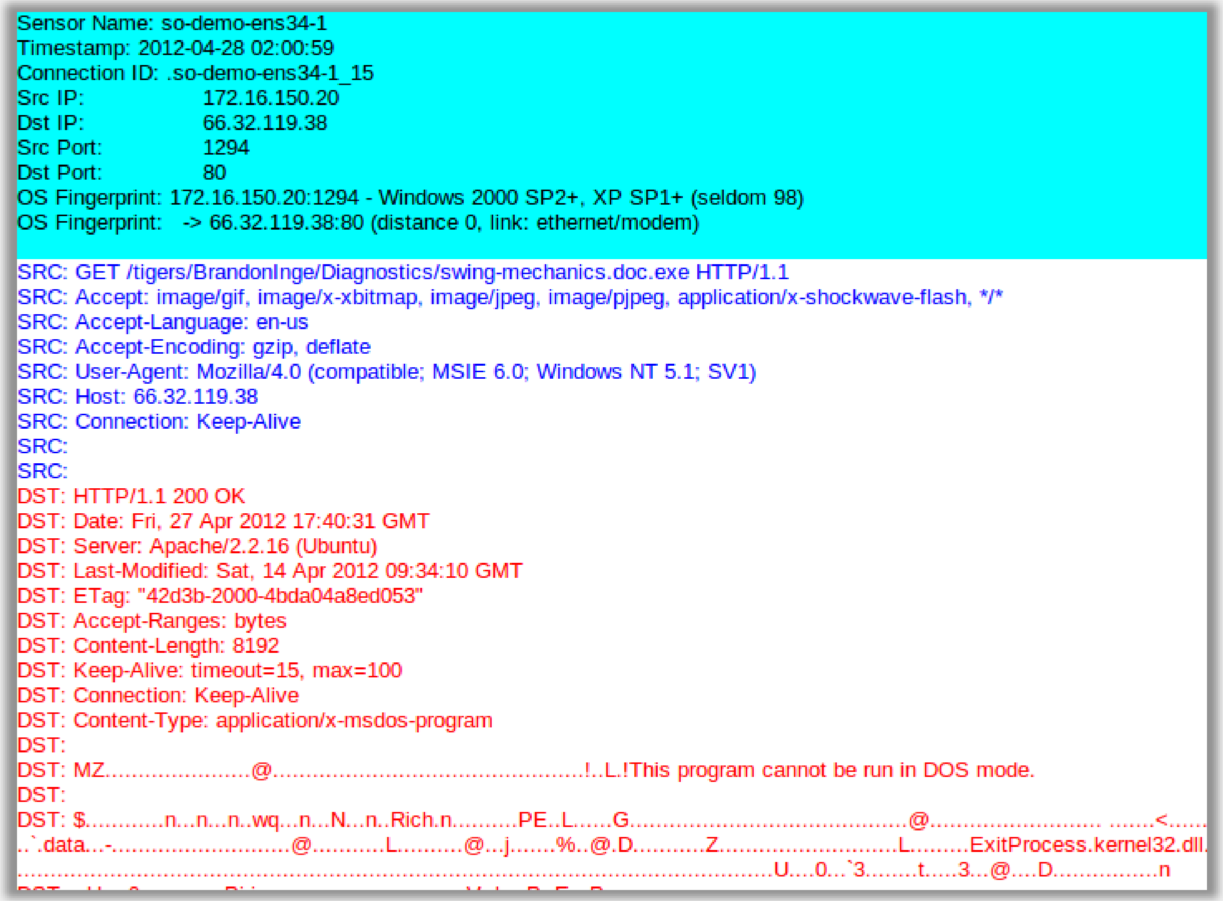
SECURITY ONION – EXTRACTED CONTENT



t	_type	doc
t	analyzer	PE, EXTRACT, SHA1, MD5
#	depth	0
□	destination_ip	172.16.150.20
t	destination_ips	172.16.150.20
#	duration	0.005689
t	event_type	bro_files
t	extracted	/nsm/bro/extracted/HTTP-FQhD1QkAbglllACSi.exe
◑	extracted_cutoff	false
□	file_ip	66.32.119.38
t	fuid	FQhD1QkAbglllACSi
t	host	gateway
t	ips	172.16.150.20
t	is_orig	false
t	local_orig	false
#	logstash_time	0.082
t	md5	e2c33fa7a3802289d46a7c3e4e1df342
t	message	{"ts":"2018-09-26T13:55:32.722724Z","fuid":"FQhD1QkAbglllACSi","tx_hosts":["66.32.119.38"],"rx_hosts":["172.16.150.20"] ["PE","EXTRACT","SHA1","MD5"],"mime_type":"application/x-dosexec","duration":0.005689,"local_orig":false,"is_orig":fals 0,"timedout":false,"md5":"e2c33fa7a3802289d46a7c3e4e1df342","sha1":"d8fd563fbbdea43c78841ccca49e8c5a3fe47cbc","extracte e}
t	mimetype	application/x-dosexec

- EXEs, etc. extracted from network traffic for future analysis
- Send to Cuckoo Sandbox, FSF (File Scanning Framework), or Strelka
- Be cautious about types of files to extract (performance-wise)

SECURITY ONION – FULL CONTENT

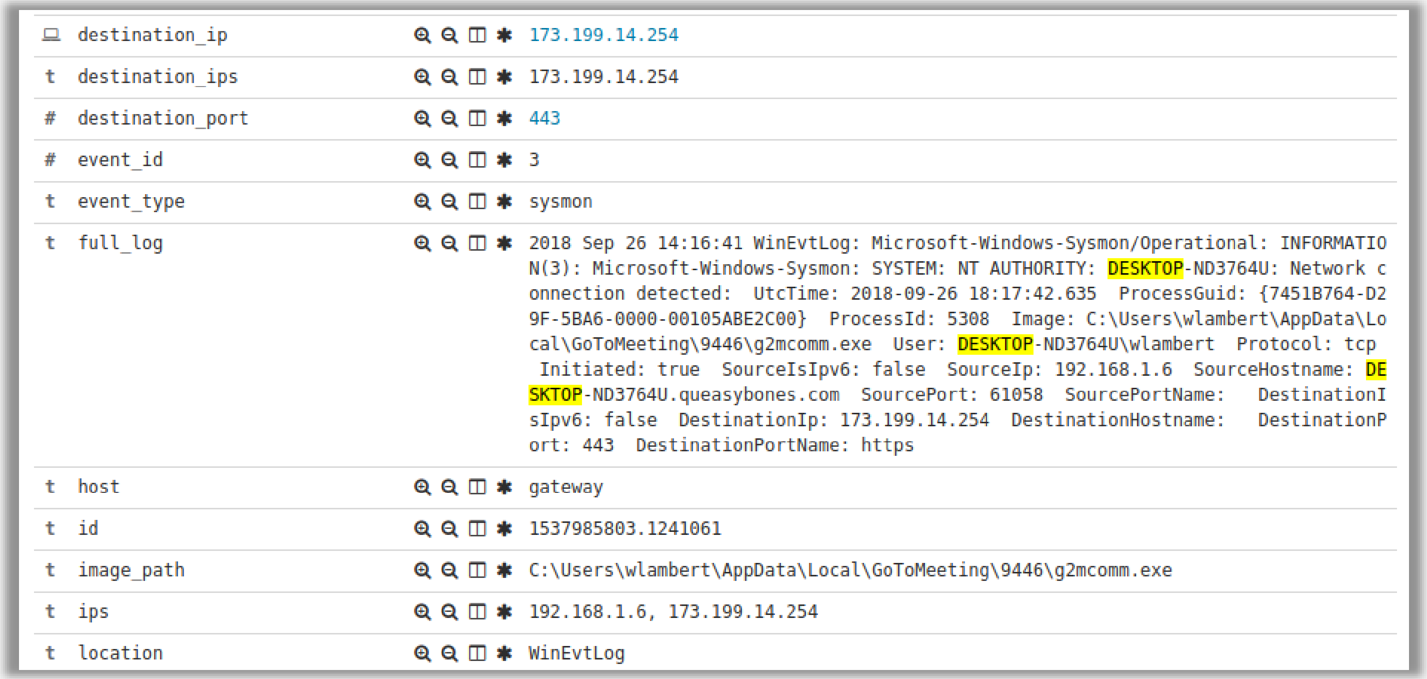


```
Sensor Name: so-demo-ens34-1
Timestamp: 2012-04-28 02:00:59
Connection ID: .so-demo-ens34-1_15
Src IP:             172.16.150.20
Dst IP:             66.32.119.38
Src Port:           1294
Dst Port:           80
OS Fingerprint: 172.16.150.20:1294 - Windows 2000 SP2+, XP SP1+ (seldom 98)
OS Fingerprint:   -> 66.32.119.38:80 (distance 0, link: ethernet/modem)

SRC: GET /tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe HTTP/1.1
SRC: Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
SRC: Accept-Language: en-us
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
SRC: Host: 66.32.119.38
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 27 Apr 2012 17:40:31 GMT
DST: Server: Apache/2.2.16 (Ubuntu)
DST: Last-Modified: Sat, 14 Apr 2012 09:34:10 GMT
DST: ETag: "42d3b-2000-4bda04a8ed053"
DST: Accept-Ranges: bytes
DST: Content-Length: 8192
DST: Keep-Alive: timeout=15, max=100
DST: Connection: Keep-Alive
DST: Content-Type: application/x-msdos-program
DST:
DST: MZ.......................@................................................!..L.!This program cannot be run in DOS mode.
DST:
DST: $............n...n...n..wq...n...N...n..Rich.n..........PE..L......G.........................................@........................ ........<......
..`.data...-..........................@...........L..........@...j.......%..@.D...........Z..........................L.........ExitProcess.kernel32.dll.
.........................................................................................................................U....0...`3........t.....3...@....D................n
```

- Start with alert/session/transaction data and drill-down for more context.
- Observe the entire stream of communication with generated transcripts.
- Manually carve objects out of the transcript or using something like NetworkMiner or Wireshark (against pcap) using a Security Onion analyst VM.

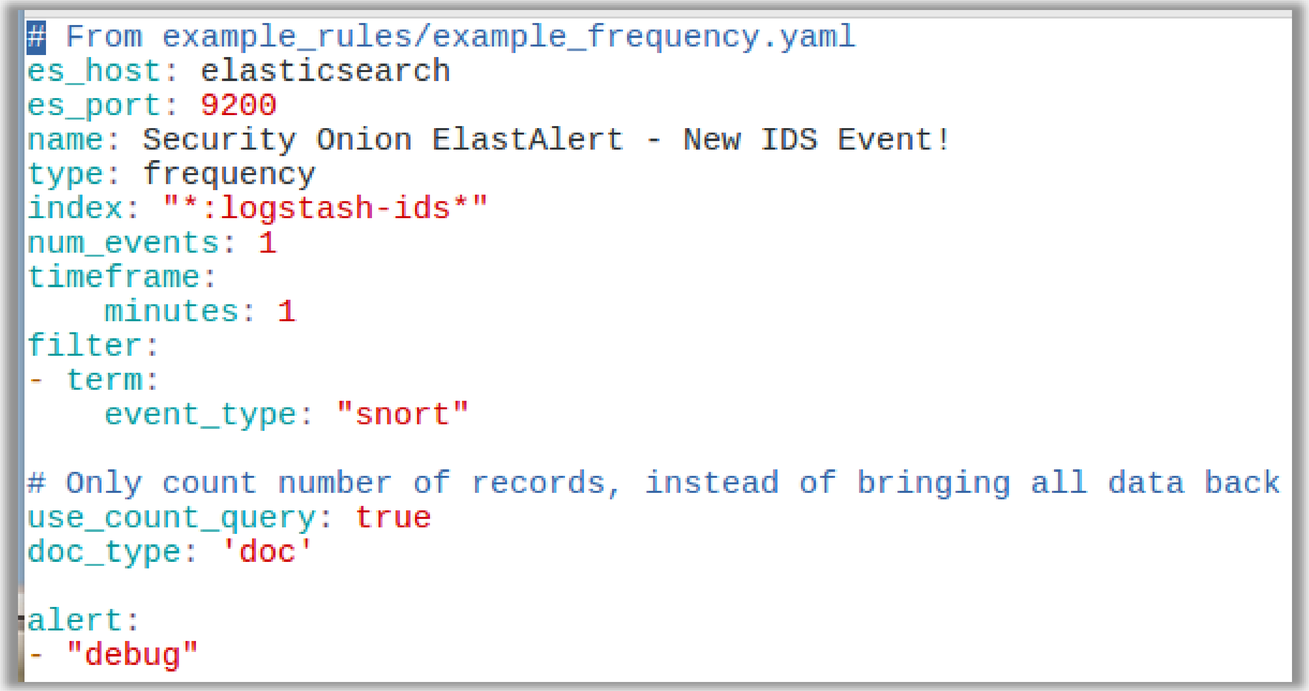
SECURITY ONION – HOST DATA

- **Wazuh** – Host-based FIM (File Integrity Monitoring), Log transport
- **Winlogbeat** – Windows Logs
- **Filebeat** – Web server logs (ISS, Apache, Nginx), Application Logs
- **Sysmon** (via Wazuh/WLB)
- **Autoruns** (via Wazuh/WLB)
- **OSQuery** (not native at the moment)



	destination_ip	173.199.14.254
t	destination_ips	173.199.14.254
#	destination_port	443
#	event_id	3
t	event_type	sysmon
t	full_log	2018 Sep 26 14:16:41 WinEvtLog: Microsoft-Windows-Sysmon/Operational: INFORMATION(3): Microsoft-Windows-Sysmon: SYSTEM: NT AUTHORITY: DESKTOP-ND3764U: Network connection detected: UtcTime: 2018-09-26 18:17:42.635 ProcessGuid: {7451B764-D29F-5BA6-0000-00105ABE2C00} ProcessId: 5308 Image: C:\Users\wlambert\AppData\Local\GoToMeeting\9446\g2mcomm.exe User: DESKTOP-ND3764U\wlambert Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.1.6 SourceHostname: DESKTOP-ND3764U.queasybones.com SourcePort: 61058 SourcePortName: DestinationIsIpv6: false DestinationIp: 173.199.14.254 DestinationHostname: DestinationPort: 443 DestinationPortName: https
t	host	gateway
t	id	1537985803.1241061
t	image_path	C:\Users\wlambert\AppData\Local\GoToMeeting\9446\g2mcomm.exe
t	ips	192.168.1.6, 173.199.14.254
t	location	WinEvtLog

SECURITY ONION - ALERTING

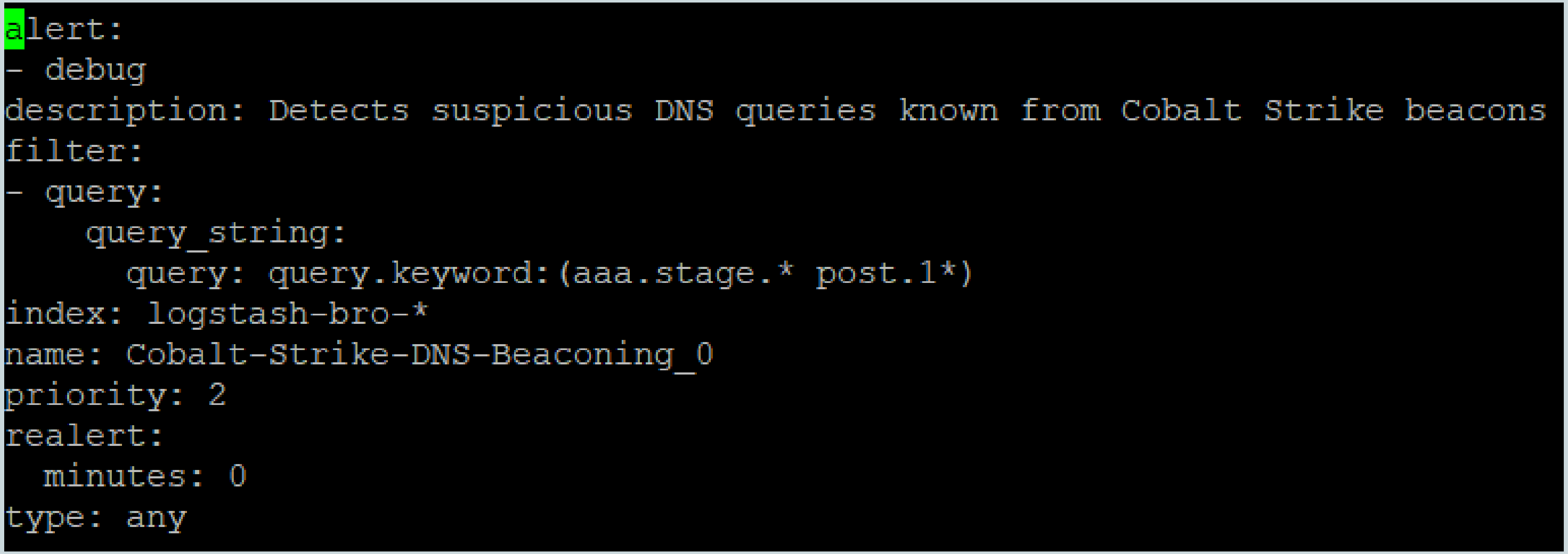


```
# From example_rules/example_frequency.yaml
es_host: elasticsearch
es_port: 9200
name: Security Onion ElastAlert - New IDS Event!
type: frequency
index: "*:logstash-ids*"
num_events: 1
timeframe:
    minutes: 1
filter:
- term:
    event_type: "snort"

# Only count number of records, instead of bringing all data back
use_count_query: true
doc_type: 'doc'

alert:
- "debug"
```

- Provides mechanism to extend information gathered to another platform for notification or analysis
- Email
- Elastalert – create a rule to trigger
  - Email
  - Slack
  - JIRA
  - Python script(s)

SECURITY ONION – SIGMA ALERTING

- Use sigmac.py to convert standard Sigma rules to a format Security Onion understands
- Implement Sigma rules via Elastalert
- Could also add in MITRE ATT&CK Techniques/IDs

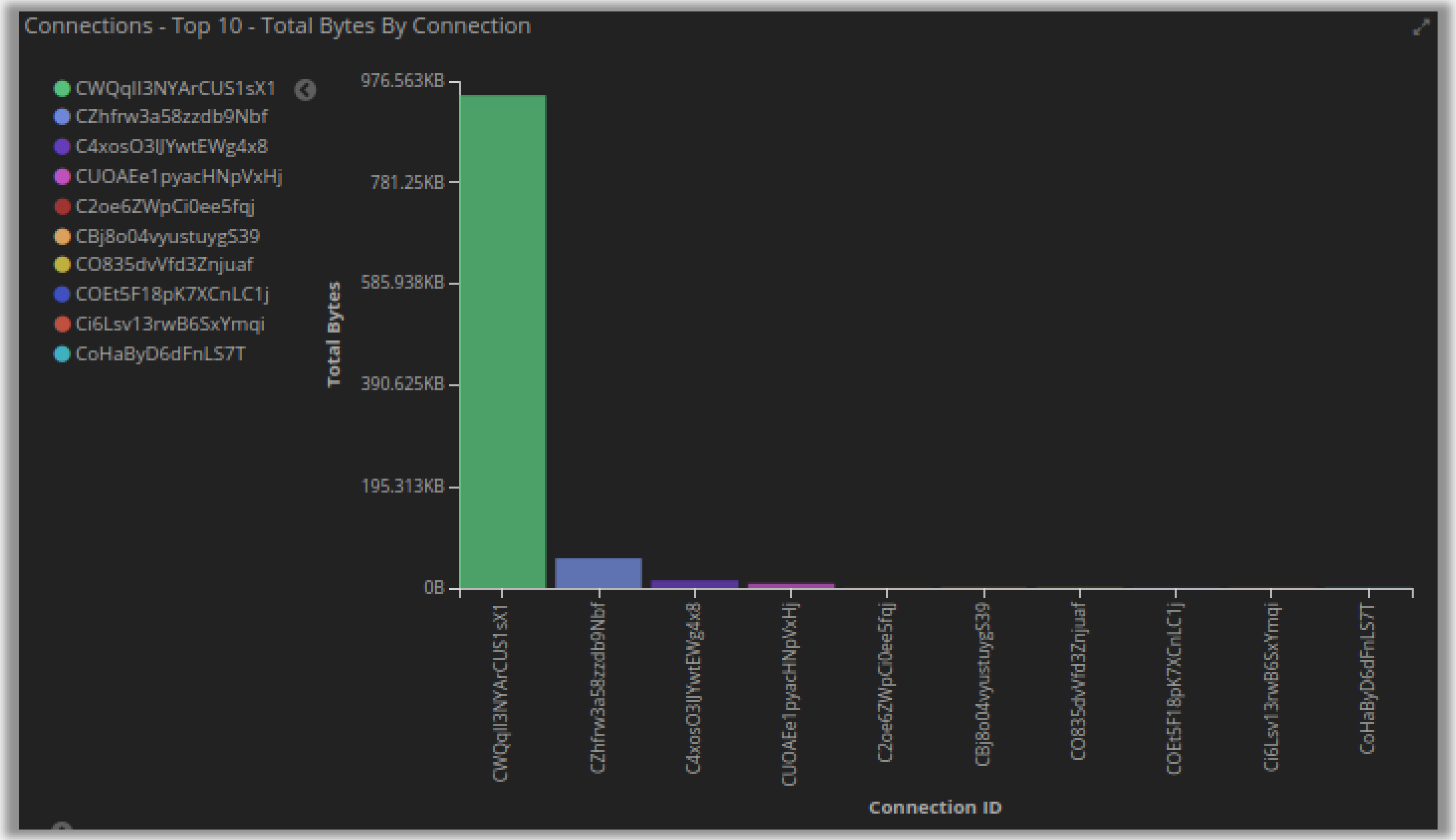


```
alert:
- debug
description: Detects suspicious DNS queries known from Cobalt Strike beacons
filter:
- query:
    query_string:
      query: query.keyword:(aaa.stage.* post.1*)
index: logstash-bro-*
name: Cobalt-Strike-DNS-Beaconing_0
priority: 2
realert:
  minutes: 0
type: any
```

https://github.com/weslambert/securityonion-sigma

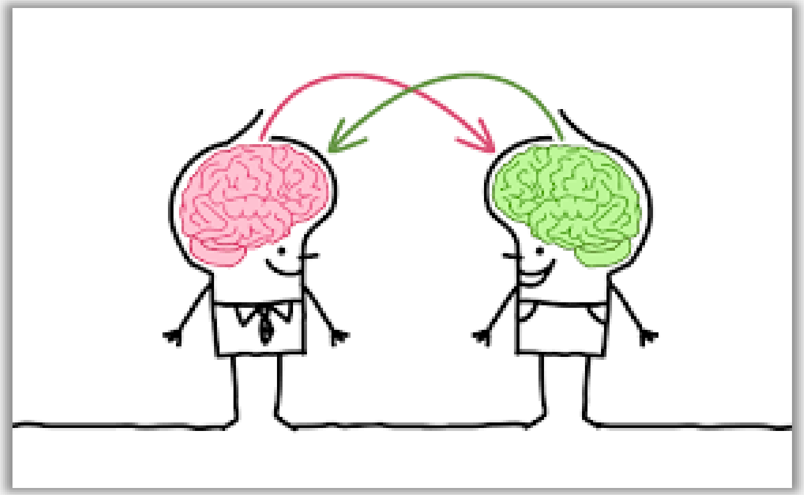
SECURITY ONION – ENRICHMENT AND VISUALIZATION

- Enrich records with GeoIP and other plugins info in Logstash pipeline
- Create custom enrichment aligning with corporate IT inventory or data
- Visualize data and correlations in Kibana
- Get to answers faster



Connections - Top 10 - Total Bytes By Connection

MISP

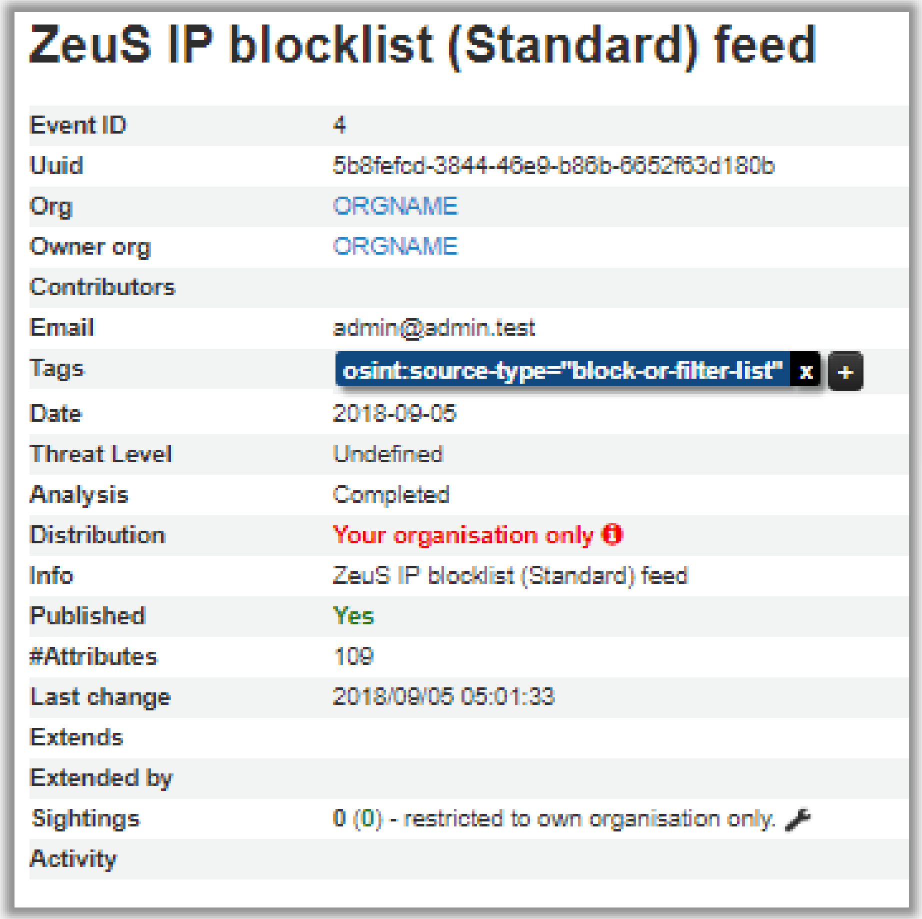


- Platform for sharing threat intel
- Provides correlation of IOCs/events
- Ability to import/export various types of data w/ a feature-rich API (integrations galore!)

MISP Threat Sharing

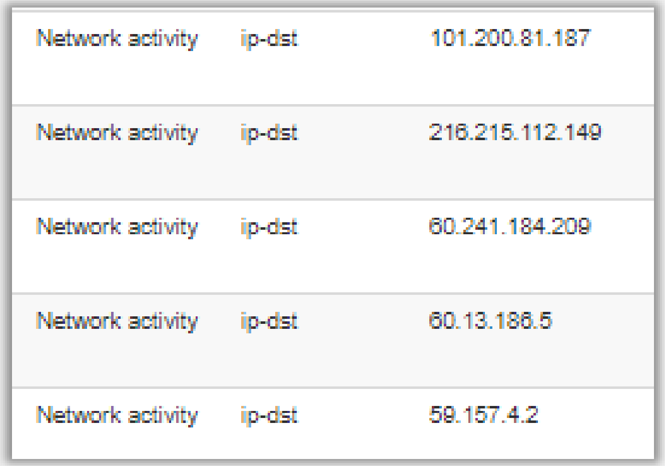
https://misp-project.org/

MISP - EVENT



ZeuS IP blocklist (Standard) feed

Event ID	4
Uuid	5b8fefcd-3844-46e9-b86b-6652f63d180b
Org	ORGNAME
Owner org	ORGNAME
Contributors	
Email	admin@admin.test
Tags	osint:source-type="block-or-filter-list" x +
Date	2018-09-05
Threat Level	Undefined
Analysis	Completed
Distribution	Your organisation only
Info	ZeuS IP blocklist (Standard) feed
Published	Yes
#Attributes	109
Last change	2018/09/05 05:01:33
Extends	
Extended by	
Sightings	0 (0) - restricted to own organisation only.
Activity	



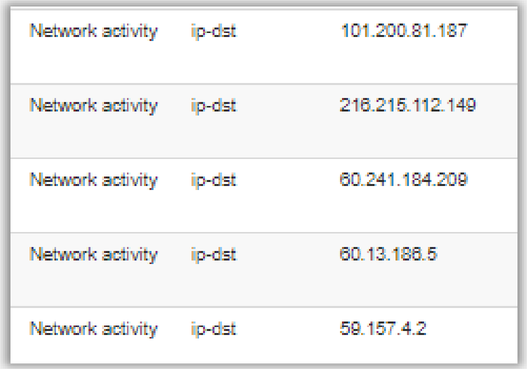
Network activity	ip-dst	101.200.81.187
Network activity	ip-dst	216.215.112.149
Network activity	ip-dst	60.241.184.209
Network activity	ip-dst	60.13.186.5
Network activity	ip-dst	59.157.4.2

Typically Contains:

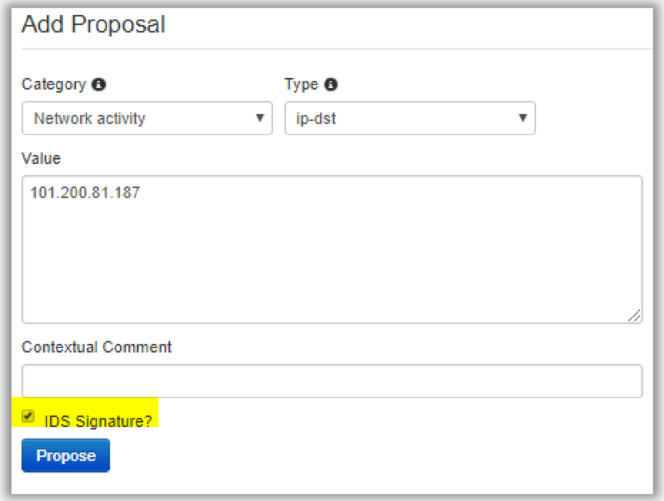
- Owner/Org
- Email
- Date
- Tags
- Info
- Threat Level
- Analysis Status
- Attributes
- Publish Status
- Sightings

MISP - ATTRIBUTES

- An event can contain several, if not, many attributes (and of different types).
- Correlation can be performed among events and their attributes.
- Can be a source/destination IP address, hash, registry key, filename, etc.



Network activity	ip-dst	101.200.81.187
Network activity	ip-dst	216.215.112.149
Network activity	ip-dst	60.241.184.209
Network activity	ip-dst	60.13.186.5
Network activity	ip-dst	59.157.4.2



Add Proposal

Category: Network activity ▾

Type: ip-dst ▾

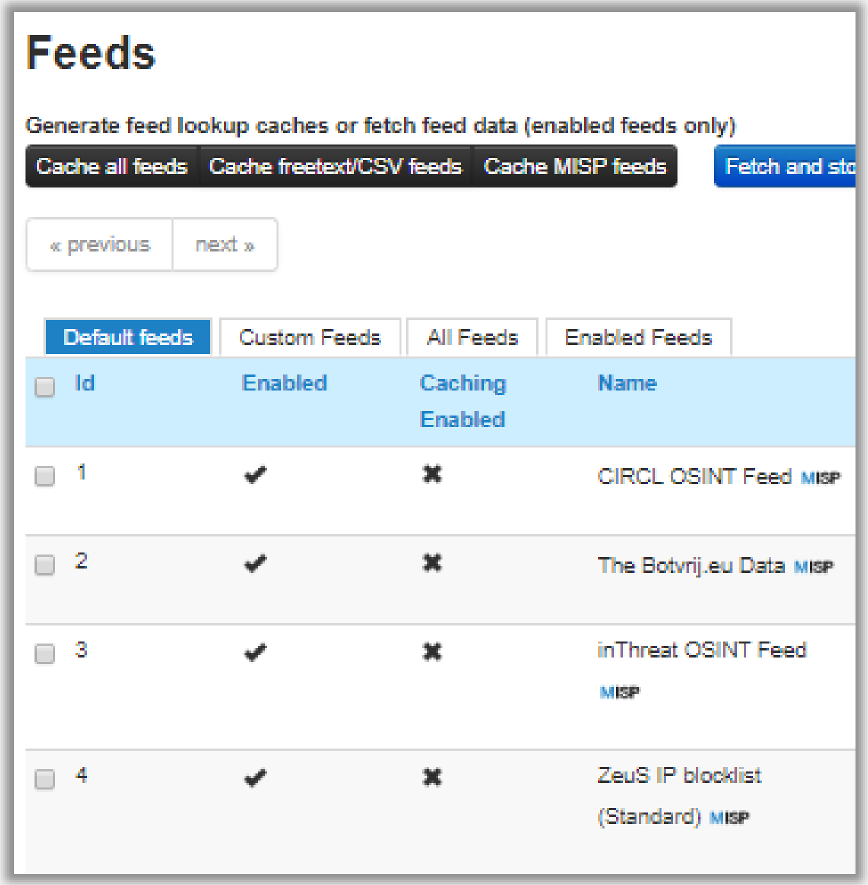
Value: 101.200.81.187

Contextual Comment:

☑ IDS Signature?

MISP - FEEDS

- HUGE list of default feeds available, including:
  - ZeuS IP blocklist (Standard)
  - Malwaredomainlist
  - Phishtank
- Integrate custom feeds
- Utilize feed attributes in IDS signatures

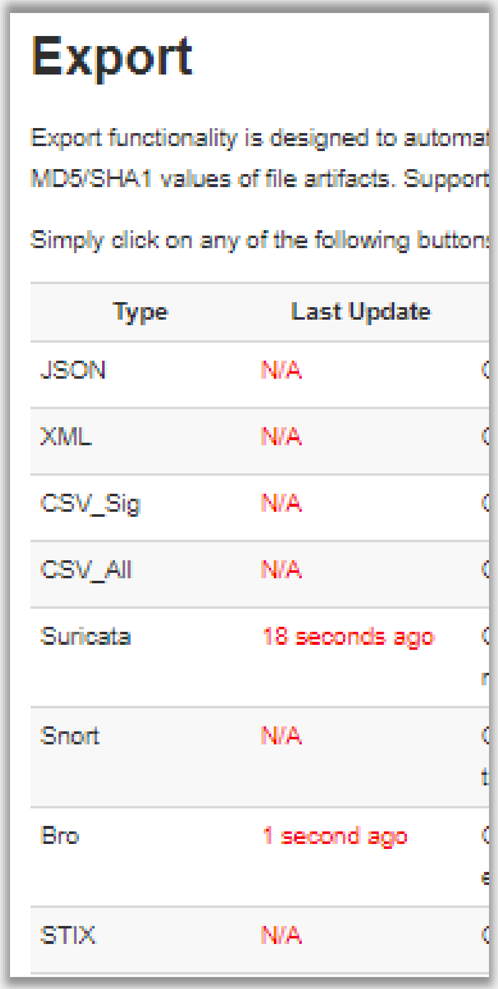


Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

□	Id	Enabled	Caching Enabled	Name
□	1	✓	✖	CIRCL OSINT Feed MISP
□	2	✓	✖	The Botvrij.eu Data MISP
□	3	✓	✖	inThreat OSINT Feed MISP
□	4	✓	✖	ZeuS IP blocklist (Standard) MISP

MISP - SIGNATURES



Export

Export functionality is designed to automat

MD5/SHA1 values of file artifacts. Support

Simply click on any of the following button

Type	Last Update
JSON	N/A
XML	N/A
CSV_Sig	N/A
CSV_All	N/A
Suricata	18 seconds ago
Snort	N/A
Bro	1 second ago
STIX	N/A

- Export IDS signatures generated by attributes from feeds or your own added attributes and use them with Snort or Suricata
- Export Bro Intel data to feed in to the Bro Intel Framework

Zeus Blocklist:

```
alert ip $HOME_NET any-> 101.200.81.187 any (msg: "MISP e4 [] Outgoing To IP: 101.200.81.187";
classtype:trojan-activity; sid:4000041; rev:1; priority:4; reference:url,/events/view/4;)
```

MISP - API

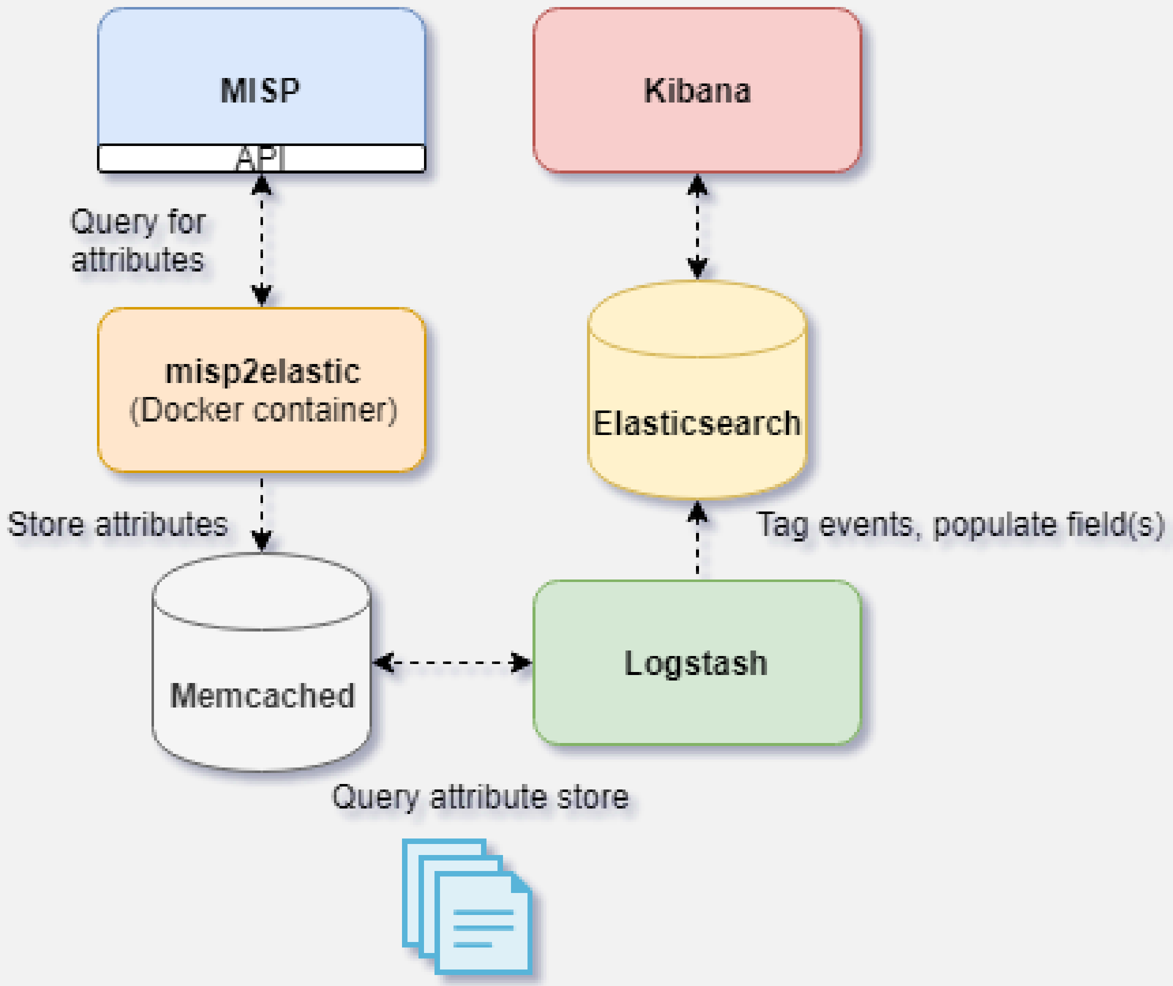
- PyMISP (client)
- Automation
  - NIDS Export (Snort/Suricata + Bro)
  - Elasticsearch enrichment
  - Add sightings
  - Manage users
  - Get/search/delete event data

MISP
Threat Sharing

MISP – ELASTICSEARCH ENRICHMENT

- Interact with MISP API to look for attribute matches
- Utilize local Memcached instance for caching
- Have Logstash perform lookup in Memcached
- Populate log events with correlated threat data

MISP – ELASTICSEARCH ENRICHMENT: FLOW

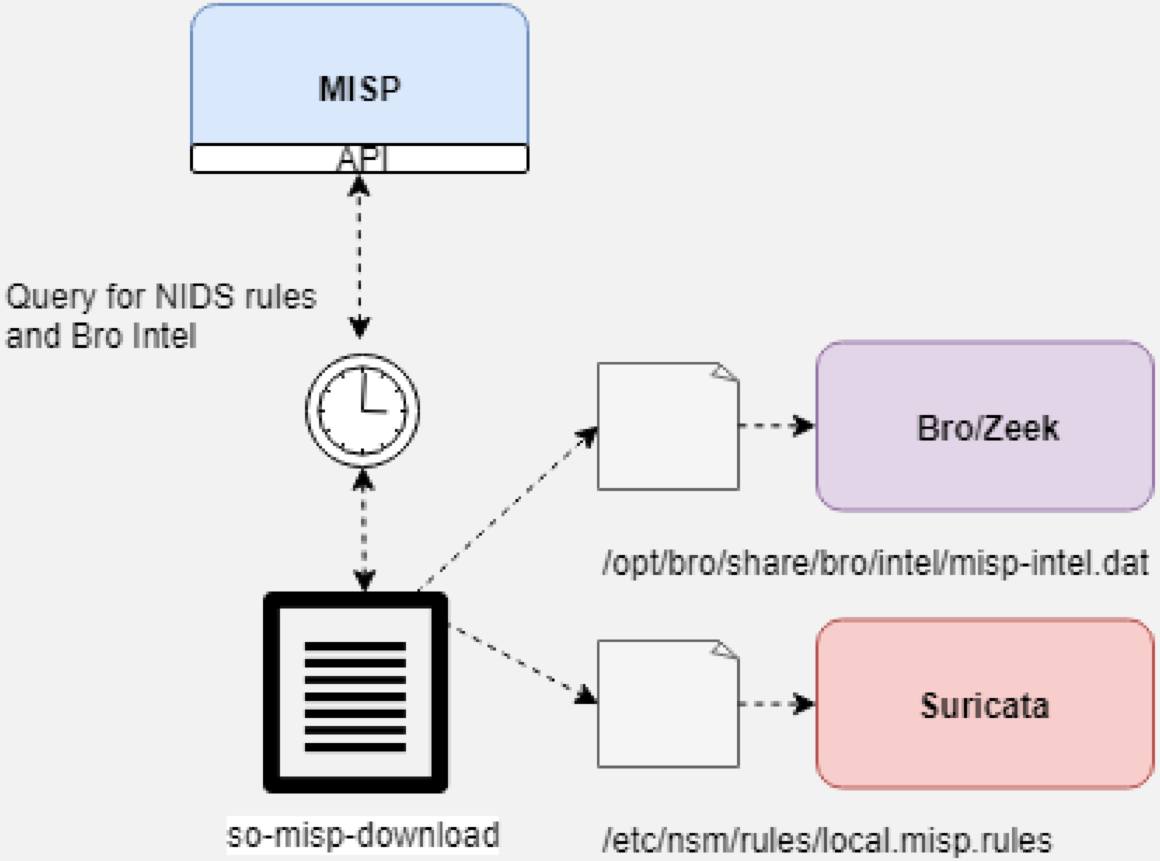


MISP – NIDS RULES/BRO INTEL

- Interact with MISP export API to export Snort/Suricata rules and/or Bro intel
- Add Snort/Suricata rules to Security Onion's local rules (misp.rules)
- Populate Bro's intel.dat with intel from MISP

https://securityonion.readthedocs.io/en/latest/misp.html?#nids-rules

MISP – NIDS RULES/BRO INTEL: FLOW

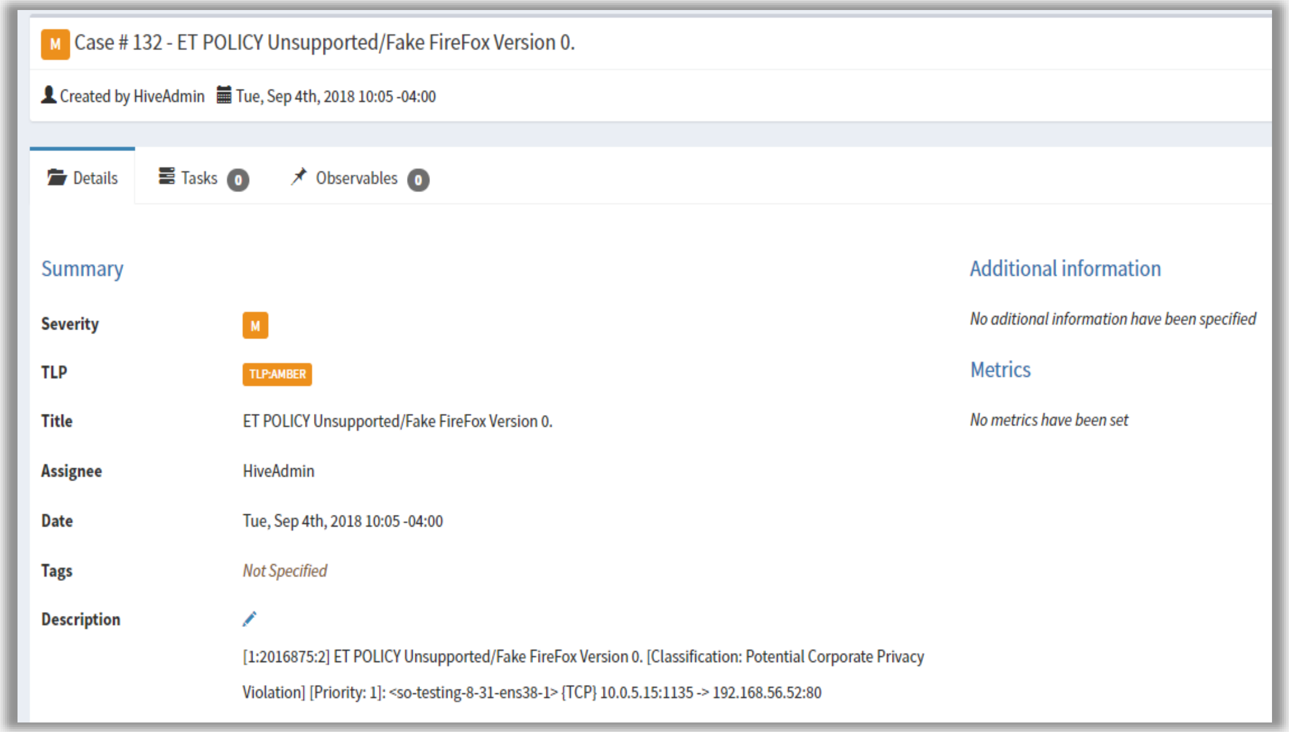

MISP
API
Query for NIDS rules and Bro Intel
Bro/Zeek
/opt/bro/share/bro/intel/misp-intel.dat
Suricata
so-misp-download
/etc/nsm/rules/local.misp.rules

THE HIVE

- Security Incident Response Platform
- Used for tracking incidents and enriching cases with external data
- Integrates well with MISP
- API

THE HIVE - CASES

- A declaration of investigation or something out of the ordinary
- Typically populated with information to include one or more observables
- Can assign tags or other additional information


M Case # 132 - ET POLICY Unsupported/Fake FireFox Version 0.

Created by HiveAdmin Tue, Sep 4th, 2018 10:05 -04:00

Summary

Severity	M
TLP	TLP:AMBER
Title	ET POLICY Unsupported/Fake FireFox Version 0.
Assignee	HiveAdmin
Date	Tue, Sep 4th, 2018 10:05 -04:00
Tags	*Not Specified*
Description	[1:2016875:2] ET POLICY Unsupported/Fake FireFox Version 0. [Classification: Potential Corporate Privacy Violation] [Priority: 1]: <so-testing-8-31-ens38-1> {TCP} 10.0.5.15:1135 -> 192.168.56.52:80

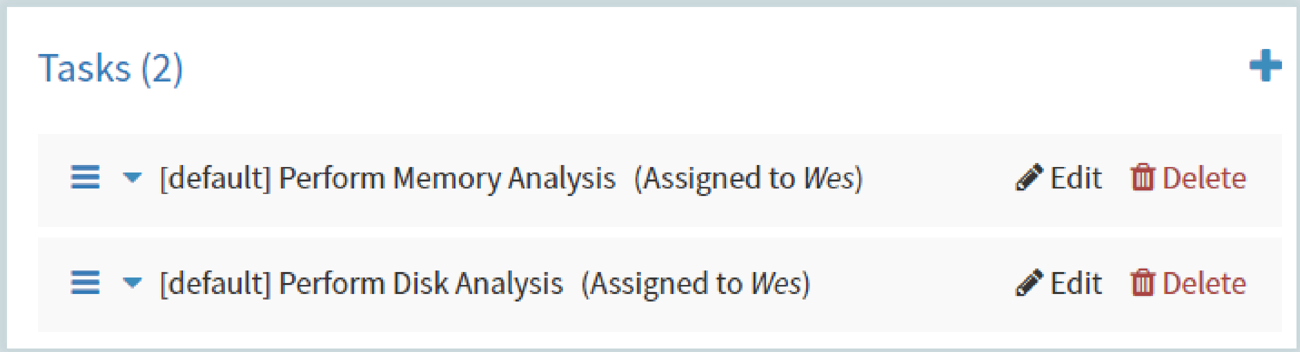
Additional information

No aditional information have been specified

Metrics

No metrics have been set

THEHIVE – CASE TEMPLATES



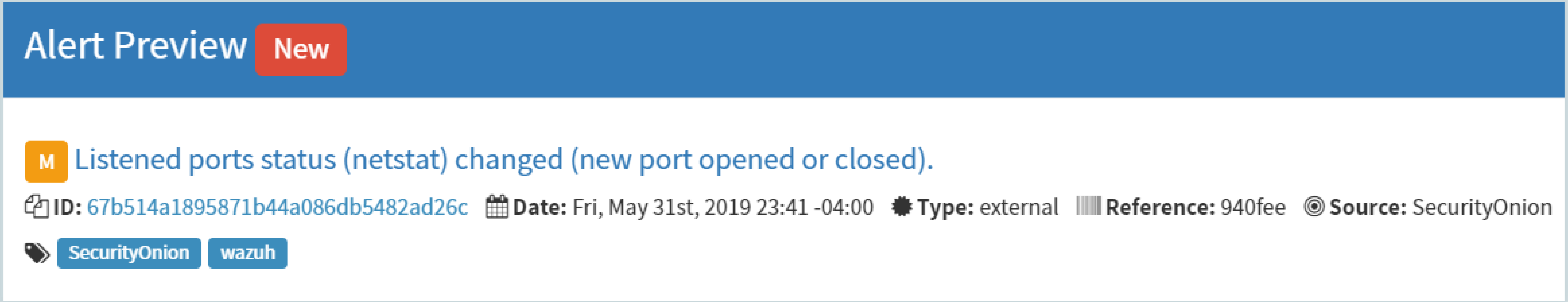
Tasks (2)

- [default] Perform Memory Analysis (Assigned to *Wes*)
- [default] Perform Disk Analysis (Assigned to *Wes*)

- Case templates allow us to define initial steps in an investigation
- Saves time
- Allows new (and even seasoned analysts) to quickly get started on investigation/remediation tasks

THEHIVE - ALERTS

- Can be generated from a noteworthy event (from external source)
- Offers a general overview of a potential threat/incident
- Can be merged into case if further investigation is needed/warranted, or can be discarded if necessary



Alert Preview New

M Listened ports status (netstat) changed (new port opened or closed).

ID: 67b514a1895871b44a086db5482ad26c Date: Fri, May 31st, 2019 23:41 -04:00 Type: external Reference: 940fee Source: SecurityOnion

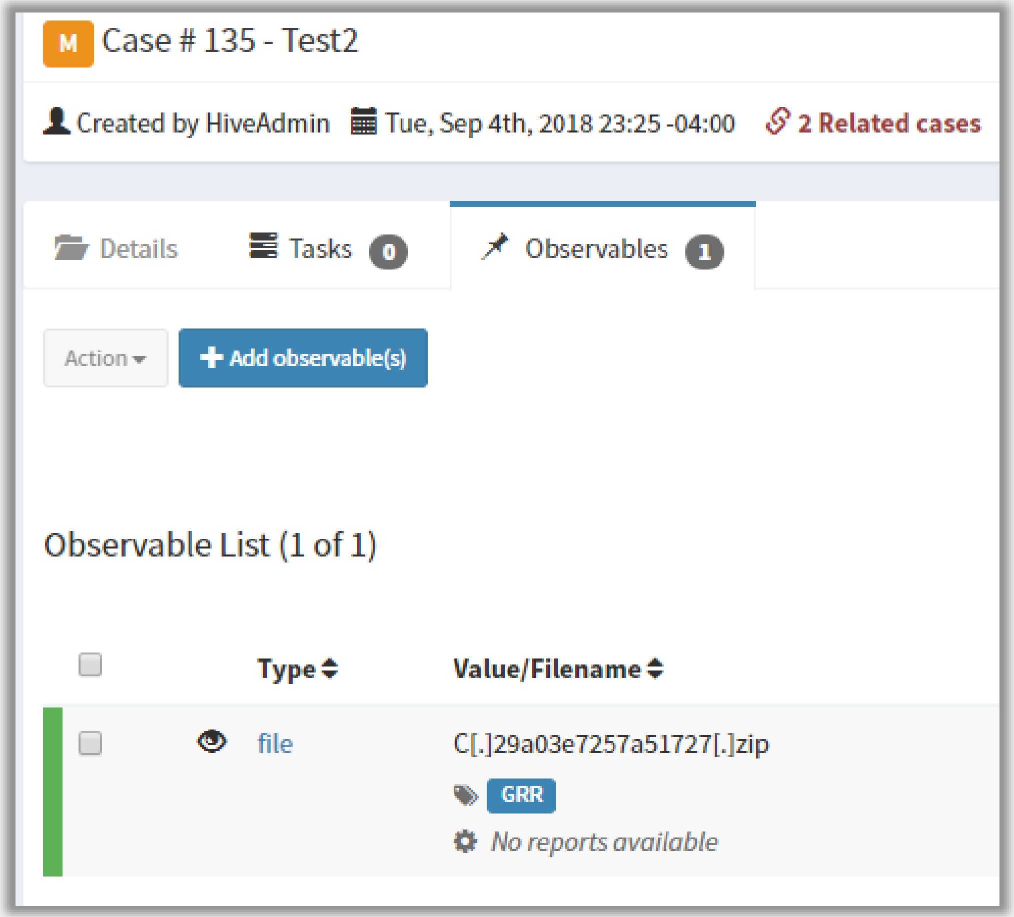
SecurityOnion wazuh

THE HIVE - OBSERVABLES

- Piece(s) of information attached to an event that can potentially be analyzed by one of the available

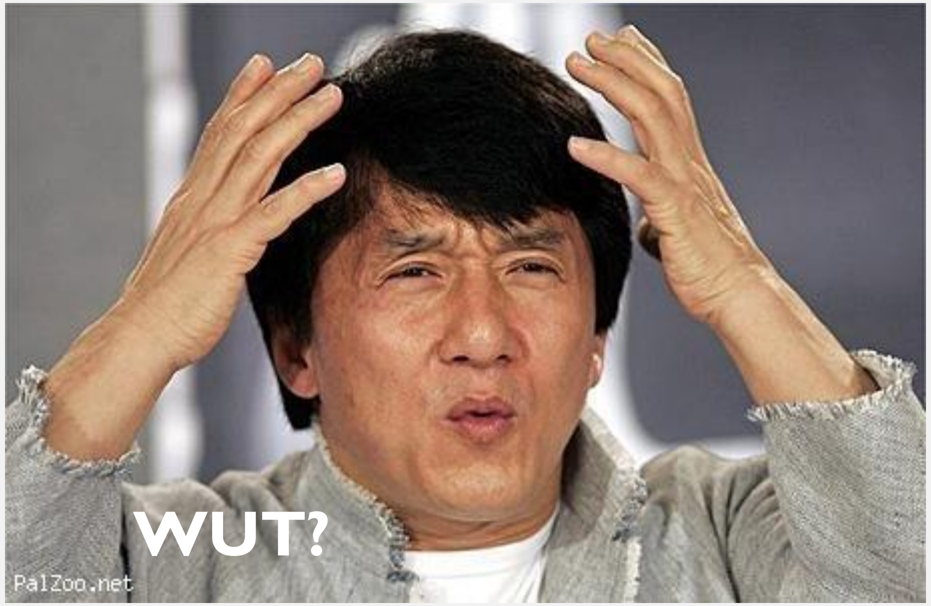
analyzers to gain greater context.

- Can be a :
  - File
  - Domain
  - IP
  - Hash
  - or something else

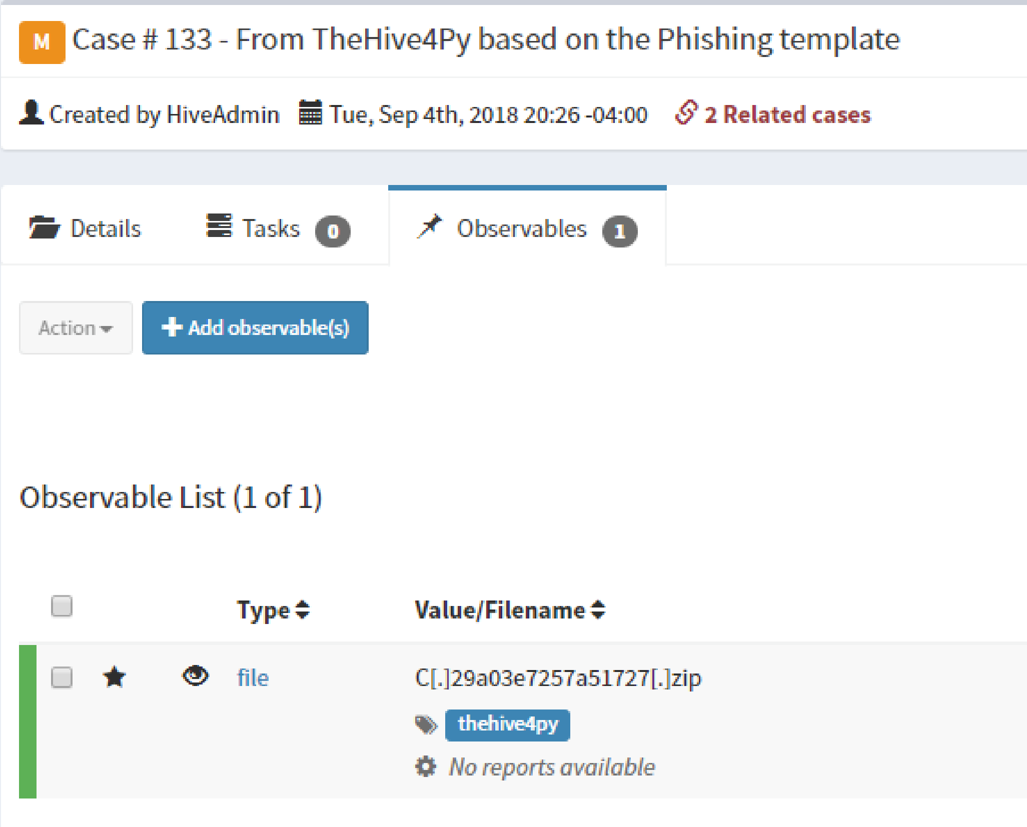


THE HIVE - ANALYZERS

- Enrich case observables with external data sources
- Analyzers include:
  - Cuckoo (file, URL analysis)
  - Dshield (reputation)
  - EmergingThreats (reputation, malware, etc.)
  - Greynoise (look for scanning activity)
  - Joe Sandbox (file analysis)
  - MISP (query MISP instances)
  - Nessus (scan hosts)
  - and many more!



THE HIVE - API



M Case # 133 - From TheHive4Py based on the Phishing template

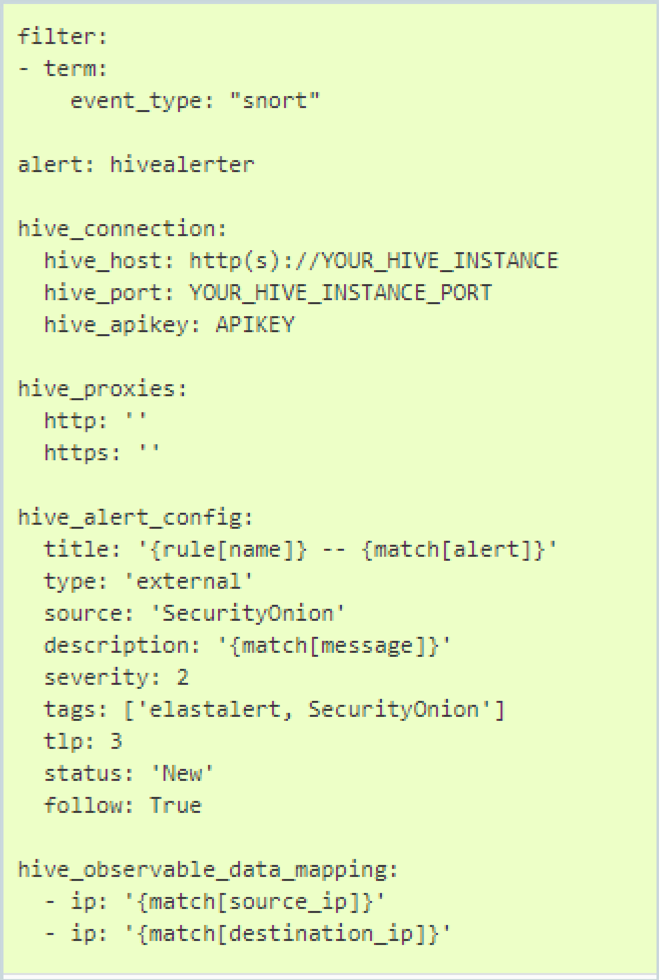
Created by HiveAdmin Tue, Sep 4th, 2018 20:26 -04:00 2 Related cases

Observable List (1 of 1)

□			Type	Value/Filename
□	★	👁	file	C[.]29a03e7257a51727[.]zip thehive4py *No reports available*

- The Hive4Py or custom Python client
  - Create a case
  - Attach observables to a case
  - Attach a task to a case
  - Raise an alert

THEHIVE - ELASTALERT

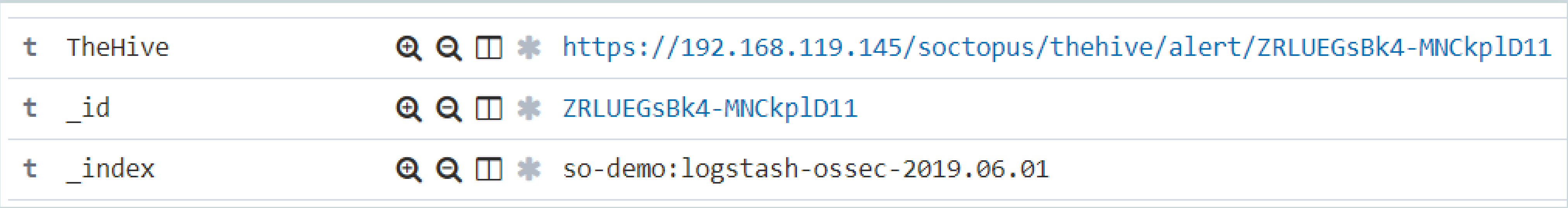


```
filter:
- term:
    event_type: "snort"

alert: hivealerter

hive_connection:
  hive_host: http(s)://YOUR_HIVE_INSTANCE
  hive_port: YOUR_HIVE_INSTANCE_PORT
  hive_apikey: APIKEY

hive_proxies:
  http: ''
  https: ''

hive_alert_config:
  title: '{rule[name]} -- {match[alert]}'
  type: 'external'
  source: 'SecurityOnion'
  description: '{match[message]}'
  severity: 2
  tags: ['elastalert, SecurityOnion']
  tlp: 3
  status: 'New'
  follow: True

hive_observable_data_mapping:
  - ip: '{match[source_ip]}'
  - ip: '{match[destination_ip]}'
```

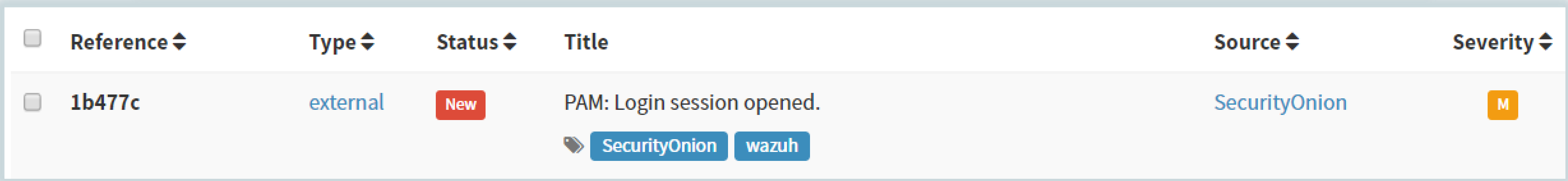
- Automatically send certain types of events to TheHive as alerts
- Define observables to attach
- For more functionality, integrate with custom Python scripting to perform other actions

https://securityonion.readthedocs.io/en/latest/hive.html

THEHIVE - SOCTOPUS



t	TheHive	https://192.168.119.145/soctopus/thehive/alert/ZRLUEGsBk4-MNCkplD11
t	_id	ZRLUEGsBk4-MNCkplD11
t	_index	so-demo:logstash-ossec-2019.06.01



□	Reference	Type	Status	Title	Source	Severity
□	1b477c	external	New	PAM: Login session opened. SecurityOnion wazuh	SecurityOnion	M

- Simple Flask API
- Click a link from Kibana to forward an event to TheHive as an alert

https://github.com/weslambert/SOCtopus

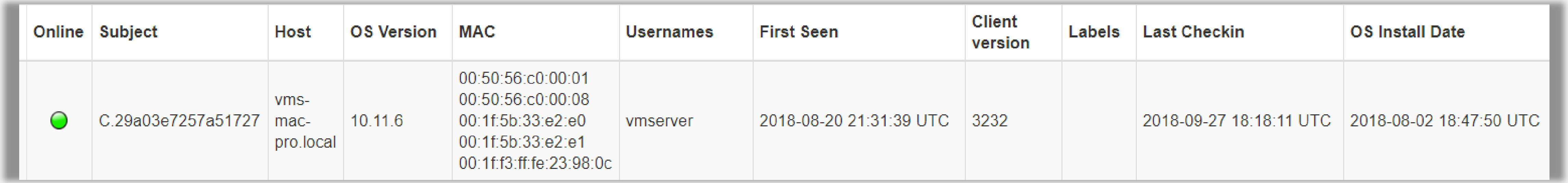
GOOGLE GRR

GRR
RAPID RESPONSE

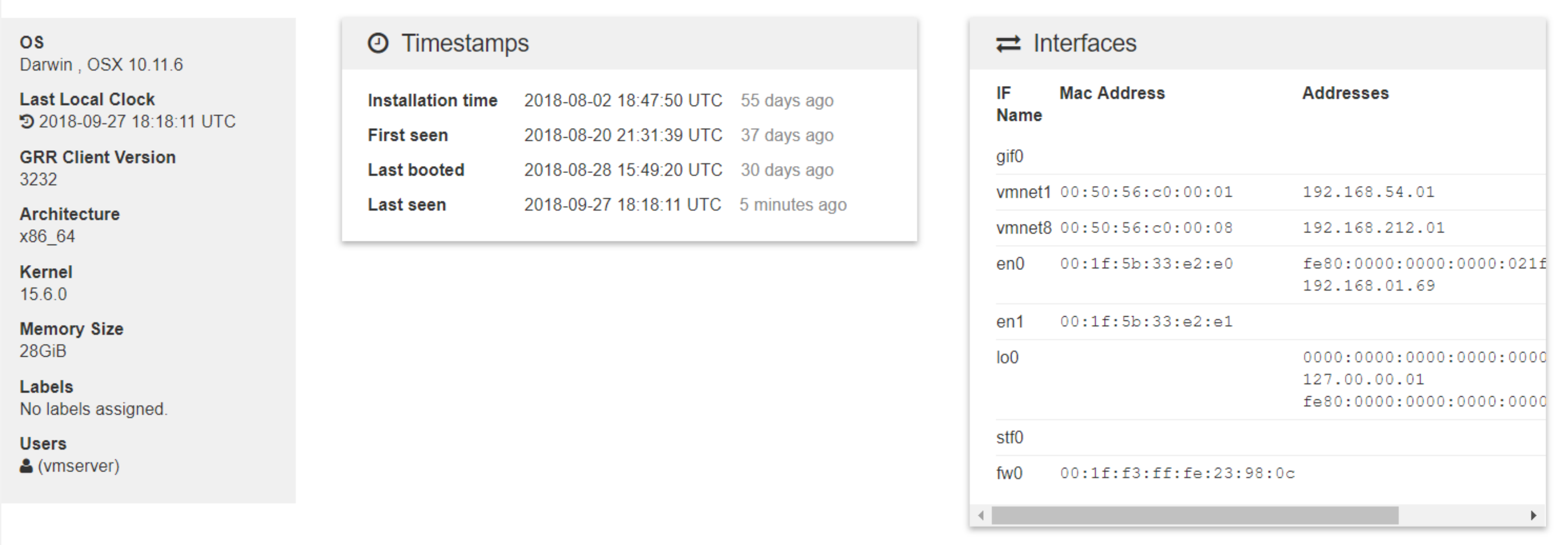
- Remote live forensics
- Quickly triage incidents and perform analysis remotely across many different hosts
- API for easy integration

https://github.com/google/grr

GRR - CLIENTS



Online	Subject	Host	OS Version	MAC	Usernames	First Seen	Client version	Labels	Last Checkin	OS Install Date
●	C.29a03e7257a51727	vms-mac-pro.local	10.11.6	00:50:56:c0:00:01 00:50:56:c0:00:08 00:1f:5b:33:e2:e0 00:1f:5b:33:e2:e1 00:1f:f3:ff:fe:23:98:0c	vmserver	2018-08-20 21:31:39 UTC	3232		2018-09-27 18:18:11 UTC	2018-08-02 18:47:50 UTC



OS
Darwin , OSX 10.11.6

Last Local Clock
2018-09-27 18:18:11 UTC

GRR Client Version
3232

Architecture
x86_64

Kernel
15.6.0

Memory Size
28GiB

Labels
No labels assigned.

Users
(vmserver)

Timestamps

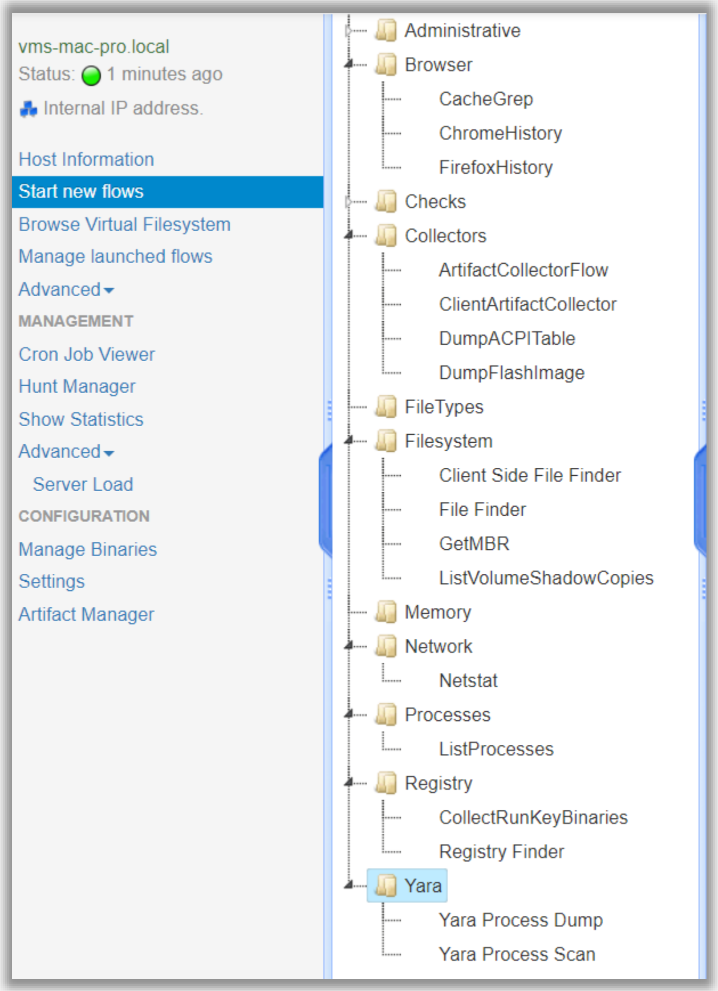
Installation time	2018-08-02 18:47:50 UTC	55 days ago
First seen	2018-08-20 21:31:39 UTC	37 days ago
Last booted	2018-08-28 15:49:20 UTC	30 days ago
Last seen	2018-09-27 18:18:11 UTC	5 minutes ago

Interfaces

IF Name	Mac Address	Addresses
gif0		
vmnet1	00:50:56:c0:00:01	192.168.54.01
vmnet8	00:50:56:c0:00:08	192.168.212.01
en0	00:1f:5b:33:e2:e0	fe80:0000:0000:0000:021f 192.168.01.69
en1	00:1f:5b:33:e2:e1	
lo0		0000:0000:0000:0000:0000 127.00.00.01 fe80:0000:0000:0000:0000
stf0		
fw0	00:1f:f3:ff:fe:23:98:0c	

- Installed on endpoints
- OS / activity info
- Allows for remote data/file retrieval/analysis
- Provides historical info

GRR - FLOW



vms-mac-pro.local
Status: ● 1 minutes ago
Internal IP address.

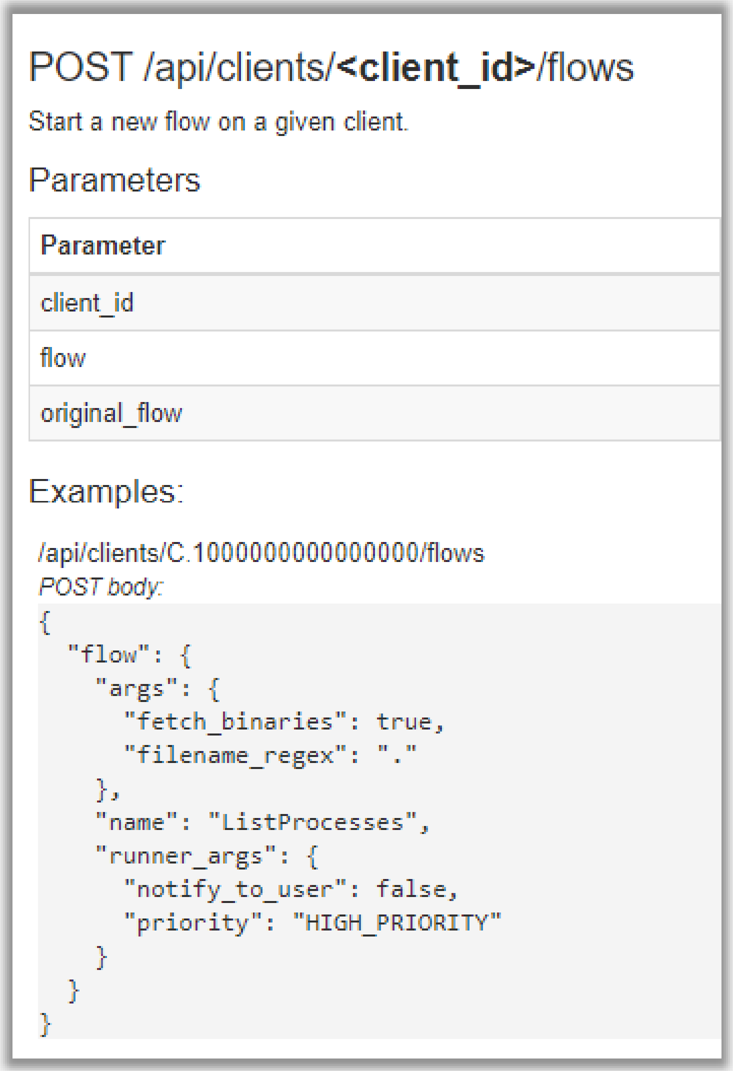
Host Information
Start new flows
Browse Virtual Filesystem
Manage launched flows
Advanced
MANAGEMENT
Cron Job Viewer
Hunt Manager
Show Statistics
Advanced
Server Load
CONFIGURATION
Manage Binaries
Settings
Artifact Manager

- Administrative
- Browser
  - CacheGrep
  - ChromeHistory
  - FirefoxHistory
- Checks
- Collectors
  - ArtifactCollectorFlow
  - ClientArtifactCollector
  - DumpACPITable
  - DumpFlashImage
- FileTypes
- Filesystem
  - Client Side File Finder
  - File Finder
  - GetMBR
  - ListVolumeShadowCopies
- Memory
- Network
  - Netstat
- Processes
  - ListProcesses
- Registry
  - CollectRunKeyBinaries
  - Registry Finder
- Yara
  - Yara Process Dump
  - Yara Process Scan

- Collect Chrome history
- Look for specific files
- List currently running processes
- List current network connections
- Scan process memory with YARA

GRR - API

- Python client library available
- Query GRR for client information
- Generate or grant approvals
- Automate the issuance of flows
- Get the results for issued flows



POST /api/clients/**<client_id>**/flows

Start a new flow on a given client.

Parameters

Parameter
client_id
flow
original_flow

Examples:

/api/clients/C.1000000000000000/flows

POST body:

```
{
  "flow": {
    "args": {
      "fetch_binaries": true,
      "filename_regex": "."
    },
    "name": "ListProcesses",
    "runner_args": {
      "notify_to_user": false,
      "priority": "HIGH_PRIORITY"
    }
  }
}
```

STRELKA

- Real-time file scanning system
- Threat hunting, detection, incident response
- Go and Python 3.6+, gRPC
- Perform file extraction and metadata collection at scale
- Great for pairing with files extracted from sensors, for example extracted files from Bro (/nsm/bro/extracted)

https://github.com/target/strelka

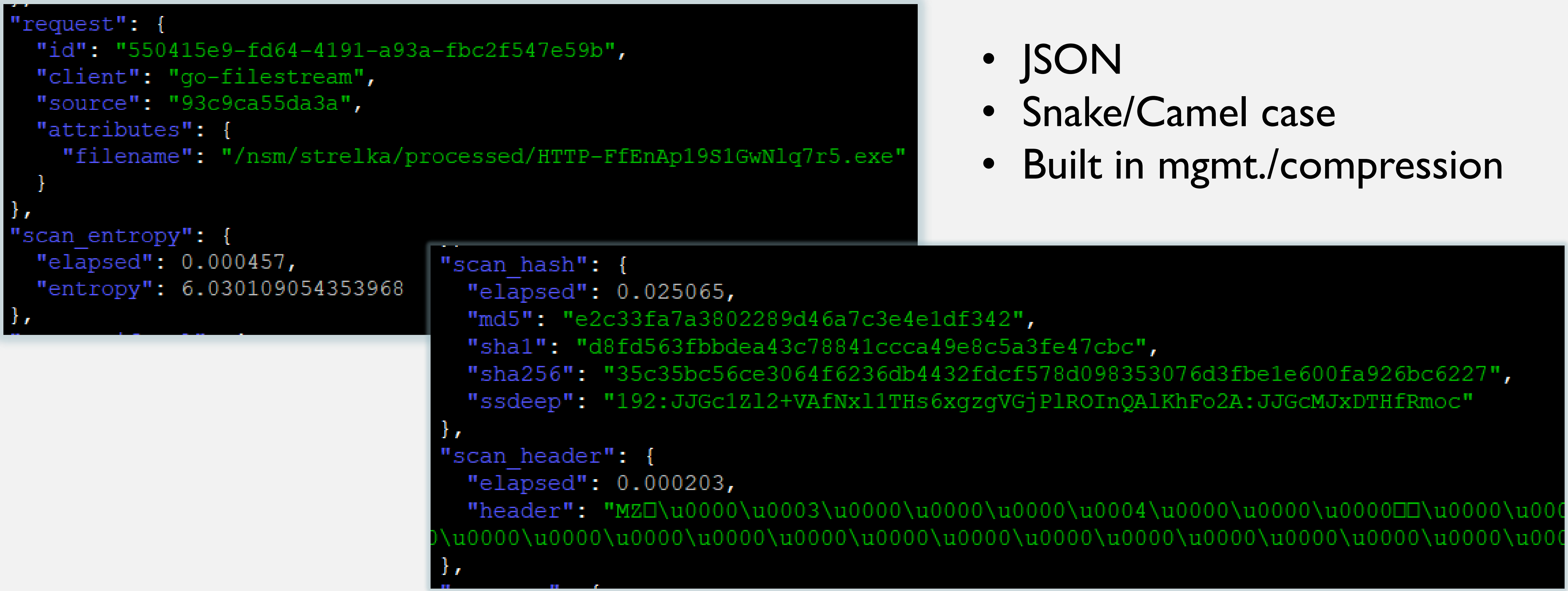
STRELKA - SCANNERS

- Scanners are assigned to files based on “flavors” and “tastes”
- Flavors
  - MIME Flavors – libmagic determines which scanners(s) to user
  - YARA flavors – YARA rule matches determine which scanner(s) to use
  - External flavors – assigned by a file request or parent file

STRELKA – USE CASES

- Extracting nested files
- Identifying malicious scripts
- Identifying suspicious executables
  - Log import functions for Mach-O and MZ files, and segments from ELF files
- Identifying suspicious text
- Interacting with external systems
  - Cuckoo Sandbox
  - MMBot – estimate maliciousness

STRELKA – SCAN RESULTS



```
"request": {
  "id": "550415e9-fd64-4191-a93a-fbc2f547e59b",
  "client": "go-filestream",
  "source": "93c9ca55da3a",
  "attributes": {
    "filename": "/nsm/strelka/processed/HTTP-FfEnAp19S1GwNlq7r5.exe"
  }
},
"scan_entropy": {
  "elapsed": 0.000457,
  "entropy": 6.030109054353968
},
```

```
"scan_hash": {
  "elapsed": 0.025065,
  "md5": "e2c33fa7a3802289d46a7c3e4e1df342",
  "sha1": "d8fd563fbbdea43c78841ccca49e8c5a3fe47cbc",
  "sha256": "35c35bc56ce3064f6236db4432fdcf578d098353076d3fbe1e600fa926bc6227",
  "ssdeep": "192:JJGc1Z12+VAfNxl1THs6xgzgVGjPlROInQAlKhFo2A:JJGcMJxDTHfRmoc"
},
"scan_header": {
  "elapsed": 0.000203,
  "header": "MZ□\u0000\u0003\u0000\u0000\u0000\u0004\u0000\u0000\u0000□□\u0000\u000
0\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u000
},
```

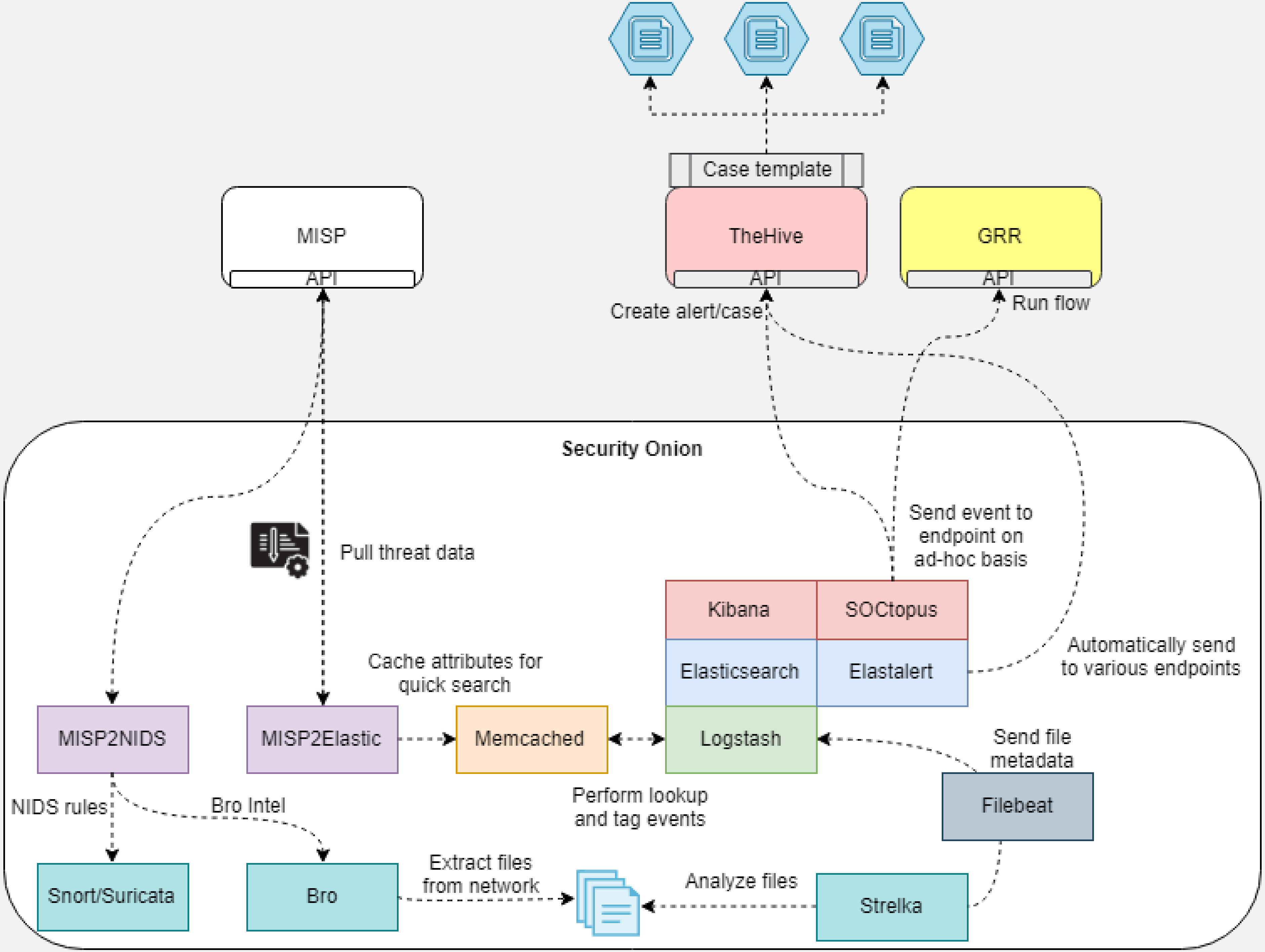
- JSON
- Snake/Camel case
- Built in mgmt./compression

STRELKA + SECURITY ONION

- Integrate with Security Onion to provide analysis of Bro's extracted files, and greater correlational capability via Kibana
- Correlate with Bro FUID to tie back to original extracted file and see relevant traffic
- Take advantage of aggregations/visualizations to quickly identify anomalies/trends

https://github.com/weslambert/securityonion-strelka

ALL TOGETHER, NOW


Case template
MISP
API
TheHive
API
GRR
API
Create alert/case
Run flow
Security Onion
Pull threat data
Send event to endpoint on ad-hoc basis
Kibana
SOCtopus
Elasticsearch
Elastalert
Automatically send to various endpoints
Cache attributes for quick search
MISP2NIDS
MISP2Elastic
Memcached
Logstash
Send file metadata
Filebeat
Perform lookup and tag events
NIDS rules
Bro Intel
Extract files from network
Analyze files
Snort/Suricata
Bro
Strelka

TOOLS

- **ElastAlert -** https://github.com/Yelp/elastalert
- **Fast IR** - https://github.com/certsocietegenerale/FIR
- **FSF -** https://github.com/EmersonElectricCo/fsf
- **Google GRR -** https://github.com/google/grr
- **MISP** - https://misp-project.org/
- **Security Onion** – https://securityonion.net
- **TheHive -** https://thehive-project.org/
- **Security Onion** – https://secruityonion.net
- **Strelka -** https://github.com/target/strelka

DROP ME A LINE

- **Twitter**:

  @therealwlambert

  @securityonion
- **Github**:

  https://github.com/weslambert